PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :		(11) Internationale Veröffentlichungsnummer:
H04L 9/32	A1	WO 98/15085
		(43) Internationales Veröffentlichungsdatum: 9. April 1998 (09.04.98)

(21) Internationales Aktenzeichen: PCT/EP97/05081

(22) Internationales Anmeldedatum: 17. September 1997 (17.09.97)

(30) Prioritätsdaten:
196 40 526.2 1. Oktober 1996 (01.10.96) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELECOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: SCHEERHORN, Alfred [DE/DE]; Ahornallee 3, D–49716 Meppen (DE). HUBER, Klaus [DE/DE]; Ernst–Ludwig–Strasse 21, D–64283 Darmstadt (DE).

(81) Bestimmungsstaaten: CA, IL, JP, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

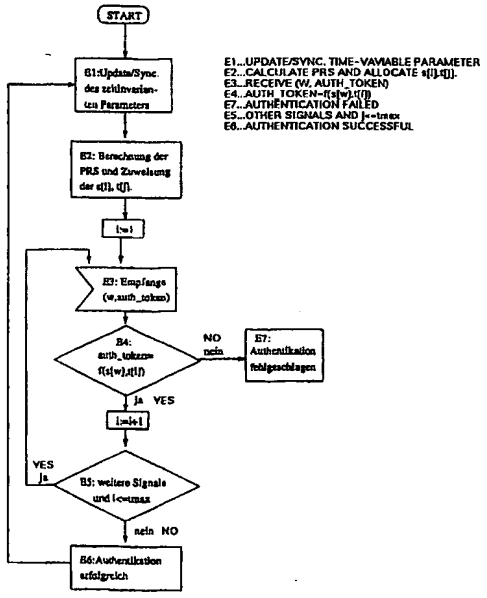
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: SIGNAL TRANSMISSION PROCESS

(54) Bezeichnung: VERFAHREN ZUR ÜBERTRAGUNG VON SIGNALEN

(57) Abstract

A process for transmitting sequences of signals/data from a transmitter to a receiver and for authenticating the sequences of signals/data consists of a precalculation phase and of a communication phase in which the signals are transmitted together with the checking sums. In the precalculation phase, a pseudo–random sequence is first generated by means of a cryptographic algorithm from a time–variable parameter and other initialisation data. Non–overlapping sections (z(1)) of a sequence (z) having each m bits are associated to signals (s(i)), wherein i = 1, 2, ... n, of a signal storage. Further non–overlapping m bit sections (t(i)) of the remaining sequence are selected for coding numbers (1, 2, ... MAX). The transmitter transmits the initialisation information and the time–variable parameters to the receiver and the receiver calculates the pseudo–random sequence (Z) and checks the received authentication token (T). The transmitter accepts the received signals as being authentic when the received authentication tokens match the calculated ones.



(57) Zusammenfassung

Das Verfahren zum Übertragen von Signal–/Datenfolgen von einem Sender zu einem Empfänger mit Authentifizierung der Signal–/Datenfolgen setzt sich aus einer Vorberechnungsphase und einer Kommunikationsphase zusammen, in der die Signale zusammen mit den Prüfsummen übertragen werden. In der Vorberechnungsphase wird mittels eines kryptographischen Algorithmus aus einem zeitvarianten Parameter und sonstigen Initialisierungsdaten zunächst eine Pseudozufallsfolge erzeugt. Aus einer Folge (z) werden sich nicht überschneidende Abschnitte (z(i)) von jeweils m Bits in Signalen (s(i)), i = 1, 2, ... n eines Signalvorrates zugeordnet. Aus der verbleibenden Folge werden weitere sich nicht überschneidende m Bit–Abschnitte (t(i)) als Codierung der Nummern (1, 2, ... MAX) gewählt. Der Sender überträgt die Initialisierungsinformation und die zeitvarianten Parameter an den Empfänger und der Empfänger berechnet seinerseits die Pseudozufallsfolge (Z) und prüft das empfangene Authentifikationstoken (T). Der Sender akzeptiert die empfangenen Signale als authentisch, wenn die vom Sender empfangenen Authentifikationstoken mit denen übereinstimmen, die er berechnet hat.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

VERFAHREN ZUR ÜBERTRAGUNG VON SIGNALEN

Die Erfindung betrifft ein Verfahren zur Übertragung von Signalen nach dem Oberbegriff des Patentanspruchs 1.

Bei der Übertragung von Signalfolgen spielt die authentische Übertragung der Daten bzw. Signale immer eine größere Rolle. So ist zum Beispiel in ISO/IEC 9797, Information technology - Security techniques - Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm (JTC1/SC27 1994) eine Lösung für dieses Problem beschrieben. Dabei sind dem Sender und dem Empfänger gleiche geheime Schlüssel in Verbindung mit einem Verschlüsselungsalgorithmus (block cipher, encipherment algorithm) oder mit einer schlüsselabhängigen Einwegfunktion (crypthgraphic check function) zugeordnet. Dies kann zum Beispiel auf einer Chipkarte erfolgen. Der Sender fügt jedem Signal (Datum) eine kryptgraphische Prüfsumme (Message authentication code) hinzu, die vom geheimen Schlüssel und dem kryptographischen Algorithmus (Verschlüsselung bzw. Einwegfunktion) abhängt. Der Empfänger berechnet seinerseits die Prüfsumme und erkennt die empfangenen Signale bei Gleichheit der Prüfsumme als authentisch an. Diese Lösung hat jedoch folgende Nachteile: Um eine Änderung der Reihenfolge der übertragenen Daten zu erkennen, wird die Prüfsumme eines Signals abhängig von der Prüfsumme der bisher gesendeten Signale berechnet. Auch für den Fall, daß nach jedem Signal eine Prüfsumme gesendet wird, ist dies notwendig, da sonst ein Angreifer Signalprüfsummenpaare aufzeichnen und in geänderter Reihenfolge unbemerkt einspielen könnte. Dies erfordert in der bekannten Lösung für jede Prüfsumme eine Durchführung des kryptographischen Algorithmus. Da Reihenfolge und

Auswahl der Signale nicht genau im Voraus feststehen, ist es auch nicht möglich, die erforderlichen Prüfsummen im Voraus zu berechnen.

In einer zeitkritischen Umgebung kann dies zu Problemen führen. Die Berechnung des kryptographischen Algorithmus kann zum Beispiel auf einer Chipkarte stattfinden. Beim Einsatz einer schon evaluierten Chipkarte ist dies vorteilhaft, ansonsten ist eine zusätzliche Softwareimplementierung des Algorithmus erneut zu evaluieren. Die Kommunikation mit der Chipkarte und die Berechnung des kryptographischen Algorithmus auf der Chipkarte sind sehr zeitintensiv.

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren zur authentischen Signal- bzw. Datenübertragung zu schaffen, das zu einem vorgegebenen Signalvorrat und einer vorgegebenen maximalen Anzahl zu übertragender Signale die Berechnung von Authentifikationsformationen vorab ermöglicht, so daß in der Übertragungsphase aus diesen schon vorher berechneten Informationen einfach und schnell Prüfsummen zu den gesendeten Signalen bzw. Daten berechnet werden können.

Die erfindungsgemäße Lösung ist im Kennzeichen des Patentanspruchs 1 charakterisiert.

Weitere Lösungen der Aufgabe bzw. Ausgestaltungen des Erfindungsgegenstandes sind in den kennzeichnenden Teilen der Patentansprüche 2 bis 10 charakterisiert.

Durch die bewußte Einführung einer Vorberechnungsphase und einer Kommunikationsphase in das Übertragungsverfahren ist es jetzt möglich, die Berechnung von Authentifikations-informationen schon vor der eigentlichen Übertragungsphase durchzuführen und während der Übertragungsphase können nun

aus diesen schon vorher berechneten Informationen einfach und schnell Prüfsummen zu den gesendeten Signalen berechnet werden. Die Lösung der Aufgabe besteht in einem Verfahren aus einer Vorberechnungsphase und einer Kommunikationsphase, in der die Signale bzw. Daten zusammen mit den Prüfsummen übertragen werden. In der Vorberechnungsphase werden mittels kryptographischer Algorithmen, zum Beispiel einer Blockchiffre im "Output-Feedback-Mode" aus dem Zeitvariantenparamenter (Sequenznummer, Zeitmarke und sonstigen Initialisierungsdaten) zunächst eine Pseudozufallsfolge Z erzeugt. Als Beispiel wird m = 16, 32 oder 64 für einen Sicherheitsparameter m angenommen. Aus der Folge Z werden jetzt sich nicht überschneidende Abschnitte z(i) von jeweils m Bit den Signalen s[i], i = 1, 2, ..., n des Signalvorrates zugeordnet. Aus der verbleibenden Folge werden weitere sich nicht überschneidende m Bit Abschnitte t[i] als Codierung der Nummern 1, 2, ... MAX gewählt, wobei MAX die maximale Anzahl der zu übertragenden Signale ist.

Wenn in der anschließenden Kommunikationsphase eine Senderauthentifikation erforderlich ist, wird zunächst dem Ablauf der "One pass authentication" gemäß den Veröffentlichungen ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication Mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994) und ISO/IEC 9798-4, Information technology - Security techniques - Entity authentication Mechanisms - Part 4: Mechanisms using a cryptographic check function (JTC1/SC27 1995) gefolgt. Der Sender überträgt die Initialisierungsformation und die zeitvarianten Parameter an den Empfänger und als Authentisierungstoken sendet er eine Anzahl bisher nicht verwendeter Bits aus Z an den Empfänger. Der Empfänger berechnet seinerseits die Pseudozufallsfolge Z und überprüft das empfangene Authentisierungstoken. Die während der Signalübertragung

vom Empfänger empfangenen Signale werden als authentisch akzeptiert, wenn die empfangenen Authentifikationstoken mit denen, die er berechnet hat, übereinstimmen. Darüberhinaus sind noch Modifikationen des Verfahrens möglich, die in der nachfolgenden Beschreibung noch im Einzelnen beschrieben werden.

Die Erfindung wird nun anhand von in der Zeichnung dargestellten Ausführungsbeispielen näher beschrieben. In der Zeichnung bedeuten:

Fig. 1 ein Flußdiagramm für die prinzipielle Operationsfolge im Empfänger und

Fig. 2 ein Flußdiagramm für die prinzipielle Operationsfolge in einem Sender.

Das Verfahren besteht aus einer Vorberechnungsphase und einer Kommunikationsphase, in der die Signale zusammen mit den Prüfsummen übertragen werden.

Vorbereitungsphase:
Mittels des kryptographischen Algorithmus (zum Beispiel einer Blockchiffre im "Output-Feedback-Mode" gemäß ISO/IEC 10116, Information Processing - Modes of Operation for an n-bit Block Cipher Algorithm (JTC1/SC27 1991)) wird aus einem zeitvarianten Parameter (Sequenznummer, Zeitmarke, gemäß ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication Mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994)) und sonstigen Initialisierungsdaten zunächst eine Pseudozufallsfolge Z erzeugt. Es sei m ein Sicherheitsparameter, zum Beispiel M = 16, 32 oder 64. Aus der Folge Z werden jetzt sich nicht überschneidende Abschnitte z[i] von jeweils m Bits den Signalen s[i], i = 1, 2, ..., n des Signalvorrates zugeordnet. Aus der

verbleibenden Folge werden weitere sich nicht überschneidende m Bit Abschnitte t[i] als Codierung der Nummern 1, 2, ...MAX gewählt, wobei MAX die maximale Anzahl der zu übertragenden Signale ist.

Kommunikationsphase:

a) Senderauthentifikation:

Falls eine Senderauthentifikation erforderlich ist, wird zunächst dem Ablauf der "One pass authentication" gemäß den Veröffentlichungen ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication Mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994) und ISO/IEC 9798-4, Information technology - Security techniques - Entity authentication Mechanisms - Part 4: Mechanisms using a crpytographic check function (JTC1/SC27 1995) gefolgt. Der Sender überträgt die Initialisierungsinformation und die zeitvarianten Parameter an den Empfänger. Als Authentisierungstoken sendet er eine Anzahl bisher nicht verwendeter Bits aus Z an den Empfänger. Der Empfänger berechnet seinerseits die Pseudozufallsfolge Z und prüft das empfangene Authentisierungstoken.

b) Signalübertragung und -authentifikation:

Sei s[k[1]] das erste Signal, das übertragen wird, dann sendet der Sender zur Authentifikation des ersten Signals T(1):=f(z[k[1]],t[1]), wobei f eine schnell berechenbare Verknüpfung der beiden Werte z[k[1]] und t[1] ist. Ein Beispiel für f ist die bitweise XOR Verknüpfung.

Für i = 2, 3, ..., i maximal MAX, sei s[k[i]] das i-te Signal, das übertragen wird. Zur Authentifikation dieses Signals sendet der Sender das Token T(i):=f(z[k[i]],t[i]). Der Empfänger führt jeweils dieselben Berechnungen aus und akzeptiert die empfangenen Signale als authentisch, wenn

die vom Sender empfangenen Authentifikationstoken mit denen, die er berechnet hat, übereinstimmen.

Die Reihenfolge der übertragenen Signale wird durch den Einfluß der Werte t[i] gesichert.

Eine Variante der Signalauthentifikation besteht im folgenden: Wenn es erforderlich ist, das Authentifikationstoken T(i) des i-ten Signals s[k[i-1]] abhängig von allen bisher gesendeten Signalen s[k[1]],...,s[k[i-1]] zu wählen, kann zur Authentifikation des i-ten Signals s[k[i]] das Token

$$T(i) = f(t[i], F(i)) \text{ gesendet werden, wobei}$$
$$F(1) = s[k[1]] \quad \text{und}$$
$$F(i) = f(s[k[i]],F(i-1)) \text{ für } i > 1.$$

Die Berechnung des Authentifikationstokens T(i) erfordert somit zweimal die Berechnung von f.

Ein Beispiel für die Anwendung eines derartigen Verfahrens ist der authentische Verbindungsaufbau beim Telefonieren. Beim Senden der Wahltöne ist nicht bekannt, ob noch ein weiterer Wahlton folgt. Deshalb erscheint es erforderlich, jeden Wahlton in der ihm nachfolgenden Pause durch die Übertragung eines Tokens zu authentisieren. Beim Mehrfrequenzwahlverfahren beträgt die Länge der Wahltöne mindestens 65ms und die Pausenlänge zwischen den Wahltönen mindestens 80ms. Mit der Authentifikation, wie sie hier beschrieben ist, ist auch diese kurze Zeitdauer von 145ms zur Authentifikation ohne Probleme möglich.

Zunächst soll anhand des Flußdiagramms nach Fig. 1 die Operations- oder Schrittfolge des Empfängers beschrieben werden.

In dem Telefonbeispiel ist der Sender das Telefon, gegebenenfalls ausgestattet mit Kryptomodul und/oder

Chipkarte, und der Empfänger das Telefonnetz, zum Beispiel die nächste Vermittlungsstelle.

E1 und S1: Hier wird der zeitinvariante Parameter zwischen dem Empfänger und Sender synchronisiert. Der zeitinvariante Parameter kann eine Sequenznummer oder Zeitmarke sein, die synchronisiert vorliegt. Dieser Parameter darf gegebenenfalls auch zur Synchronisation im Klartext oder verschlüsselt vom Sender an den Empfänger gesendet werden. Im erfindungsgemäßen Verfahren ist es sinnvoll, daß der Sender den zeitinvarianten Parameter schon kennt, bevor ein Verbindungsaufbau gewünscht wird, um die s[], t[] vorzuberechnen.

E2 und S2: Hier berechnen Sender und Empfänger zunächst eine Zufallsfolge PRS (Pseudo-Random-Sequence) der Länge $m^*(smax+tmax)$ Bit, wobei

m: Sicherheitsparameter, im Beispiel m:=32.

smax: Maximale Anzahl der unterschiedlichen Signale (Anzahl der Elemente des Alphabets/Signalvorates). Im Telefonbeispiel die Ziffern 1..9 und Spezialsymbole wie #, und andere.

tmax: Maximale Anzahl der Signale, die in einem Durchgang authentisiert werden sollen. Im Telefonbeispiel max. Länge einer Telefonnummer, max. Anzahl von Ziffern und Spezialsymbolen für einen Verbindungsaufbau.

Danach werden jeweils sich nicht überschneidende Abschnitte von m Bits dieser Zufallsfolge PRS den m Bit Größen s[1], s[2], ..., s[smax], t[1], t[2], ..., t[tmax] zugewiesen:
s[1] = Bit 1 bis Bit m der PRS
s[2] = Bit m+1 bis Bit 2^*m der PRS
...

s[max] = Bit (smax-1)*m+1 bis Bit smax*m der Zufallsfolge PRS
t[1] = Bit smax*m+1 bis Bit (smax+1)*m der Zufallsfolge PRS
t[tmax] = Bit (smax+tmax-1)*m+1 bis Bit (smax+tmax)*m der Zufallsfolge PRS

Anhand von Fig. 2 wird nachfolgend die Operations- oder Schrittfolge für den Sender beschrieben.

S3: Der Sender wartet auf ein Signal w, das authentisch übertragen werden soll. w wird als natürliche Zahl zwischen 1, 2, ..., smax interpretiert, um die Abbildung w -> s[w] einfach zu halten.

S4: Der Sender sendet das i-te Signal w zusammen mit dem Authentifizierungstoken f(s[w],t[i]). Im Telefonbeispiel ist das Token f(s[w],t[i])=s[w]+t[i], das bitweise XOR von s[w] und t[i].

S5: S3 und S4 werden solange iteriert wiederholt, bis entweder keine Signale mehr authentisch übertragen werden sollen oder die maximale Anzahl von Signalen, die mit diesem Vorrat an vorberechneter Zufallsfolge PRS authentisiert werden können, erreicht ist.

S6: Im Telefonbeispiel wartet der Sender jetzt auf den Verbindungsaufbau des Empfängers.

E3, E4 und E5: Solange neue Signale mit zugehörigen Authentisierungstoken empfangen werden, prüft der Empfänger, ob die von ihm berechneten Authentisierungstoken mit den empfangenen übereinstimmen.

E6: Falls alle Token übereinstimmen, werden die empfangenen Signale als authentisch akzeptiert. Im Telefonbeispiel erfolgt jetzt der Verbindungsaufbau.

E7: Bei nicht erfolgreicher Authentisierung erfolgt kein Verbindungsaufbau.

P A T E N T A N S P R Ü C H E

1. Verfahren zum Übertragen von Signal-/Datenfolgen zwischen einem Sender und einem Empfänger mit Authentifizierung der übertragenen Signal-/Datenfolgen durch Verwendung von Schlüsseln und kryptographischen Algorithmen, die sowohl auf der Sender- als auch auf der Empfängerseite implementiert sind, dadurch gekennzeichnet,

   daß in einer Vorberechnungsphase mittels kryptographischer Algorithmen Daten abhängig von einem geheimen Schlüssel berechnet werden, aus denen in einer nachfolgenden Übertragungsphase Authentifikationstoken für die Signale berechnet werden, die sowohl die Signale als auch die Reihenfolge des Sendens der Signale authentisieren.

2. Verfahren nach Patentanspruch 1, dadurch gekennzeichnet,

   daß in der Vorbereitungsphase mittels eines kryptographischen Algorithmus eine Pseudozufallsfolge (PRS) erzeugt wird,

   daß aus dieser Folge bestimmte Abschnitte als Codierung sowohl der Signale des Signalvorrates als auch der Sendestellen (1, 2, ... MAX) verwendet werden und

   daß das Authentifikationstoken des Signals, das an i-ter (i = 1, 2, ..., MAX) Stelle gesendet wird, abhängig von der Codierung des Signals und von der Codierung der Sendestelle (i) berechnet wird.

3. Verfahren nach Patentanspruch 2, dadurch gekennzeichnet,

daß das Authentifikationstoken (T) des Signals, das an i-ter (i = 1, 2, ..., MAX) Stelle gesendet wird, die bitweise XOR-Verknüpfung oder eine äquivalente logische Funktion der Codierung des jeweiligen Signals und der Codierung der Sendestelle (i) ist.

4. Verfahren nach Patentanspruch 1, dadurch gekennzeichnet,

daß in der Vorberechnungsphase mittels eines kryptographischen Algorithmus eine Pseudozufallsfolge (PRS) erzeugt wird,

daß aus dieser Folge bestimmte Abschnitte als Codierung sowohl der Signale des Signalvorrates als auch der Sendestellen (1, 2, ..., MAX) verwendet werden und

daß das Authentifikationstoken des Signals, das an i-ter Stelle (i = 1, 2, ..., MAX) gesendet wird, abhängig von der Codierung aller bisher gesendeten Signale (1, 2, ..., i) und von der Codierung der Sendestelle (i) berechnet wird.

5. Verfahren nach einem der Patentansprüche 1 bis 4, dadurch gekennzeichnet,

daß das Authentifikationstoken (T) des Signals, das an i-ter Stelle (i = 1, 2, ... MAX) gesendet wird, die bitweise XOR-Verknüpfung oder eine äquivalente logische Verknüpfung der Codierung aller bisher gesendeten Signale (1, 2, ... i) und der Codierung der Sendestelle (i) ist.

6. Verfahren nach einem der Patentansprüche 1 bis 5, dadurch gekennzeichnet,

daß der in der Vorberechnungsphase verwendete kryptographische Algorithmus eine Blockchiffre ist.

7. Verfahren nach Patentanspruch 6, dadurch gekennzeichnet,

daß als Blockchiffre der bekannte "Data Encryption Standard" verwendet wird.

8. Verfahren nach einem der Patentansprüche 6 bzw. 7, dadurch gekennzeichnet,

daß die Pseudozufallsfolge (PSR) durch Betreiben der Blockchiffre im bekannten "Output-Feedback-Mode" erzeugt wird.

9. Verfahren nach dem Oberbegriff des Patentanspruchs 1 bzw. nach einem der Patentansprüche 2 bis 8, dadurch gekennzeichnet,

daß in der Vorbereitungsphase zusätzlich ein Token (T) zur Authentifikation des jeweiligen Senders berechnet wird, das nachfolgend übertragen wird und den Empfänger zur Authentifikation des Senders initiiert.

10. Verfahren nach einem der Patentansprüche 1 bis 9, dadurch gekennzeichnet,

daß die Reihenfolge der übertragenen Signale durch die sich nicht überschneidenden m Bit Abschnitte (t(i)) gesichert ist.

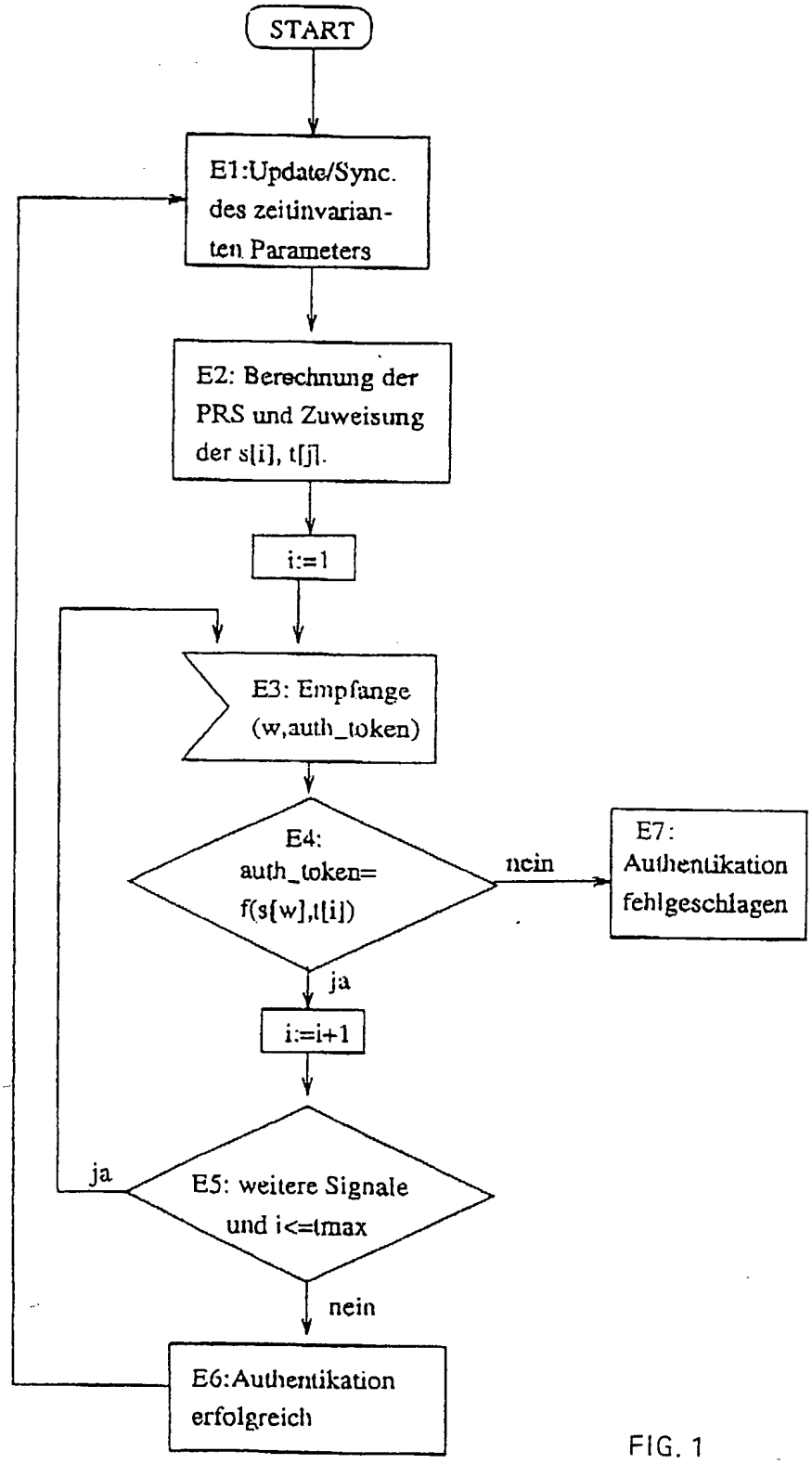

START
E1:Update/Sync. des zeitinvarianten Parameters
E2: Berechnung der PRS und Zuweisung der s[i], t[j].
i:=1
E3: Empfange (w,auth_token)
E4: auth_token= f(s[w],t[i])
nein
E7: Authentikation fehlgeschlagen
ja
i:=i+1
E5: weitere Signale und i<=tmax
ja
nein
E6:Authentikation erfolgreich

FIG. 1

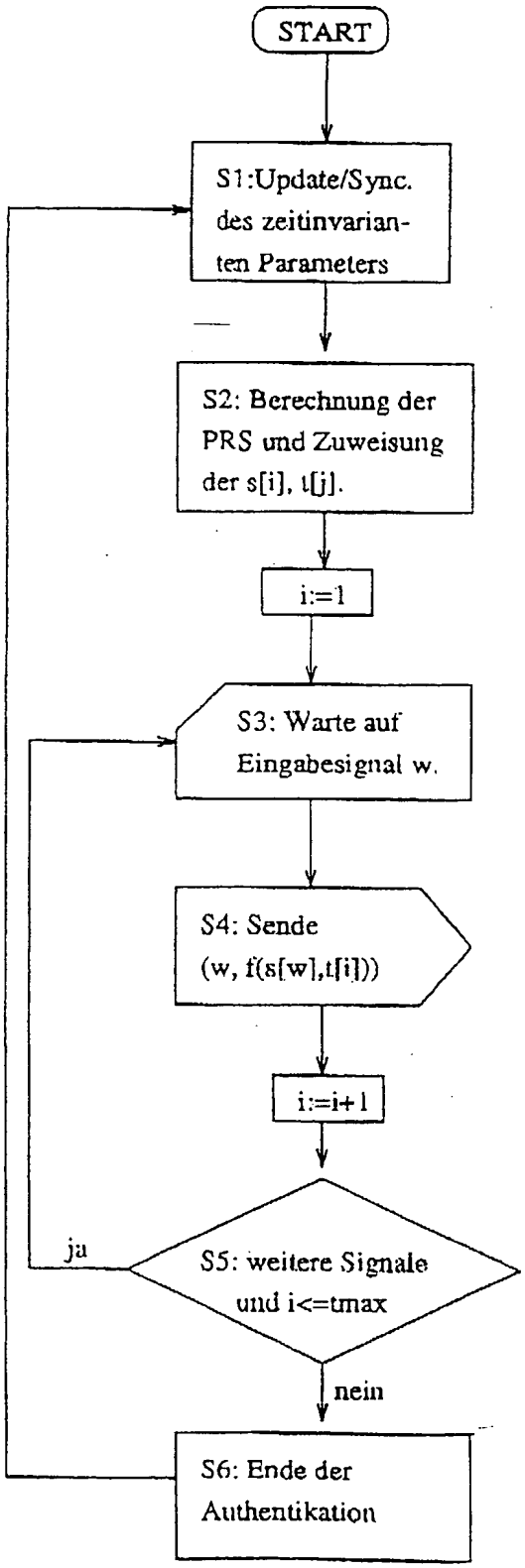

START
S1:Update/Sync. des zeitinvarianten Parameters
S2: Berechnung der PRS und Zuweisung der s[i], t[j].
i:=1
S3: Warte auf Eingabesignal w.
S4: Sende (w, f(s[w],t[i]))
i:=i+1
S5: weitere Signale und i<=tmax
ja
nein
S6: Ende der Authentikation

FIG. 2

INTERNATIONAL SEARCH REPORT

Intern. nal Application No
PCT/EP 97/05081

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimumdocumentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 94 21066 A (TELSTRA) 15 September 1994 see page 4, line 6 - line 15 see page 6, line 10 - line 17 see page 7, line 17 - page 8, line 3	1,2
A	JUENEMAN ET AL.: "MESSAGE AUTHENTICATION WITH MANIPULATION DETECTION CODES" PROCEEDINGS OF THE 1983 SYMPOSIUM ON SECURITY AND PRIVACY, 25 April 1983, SILVER SPRING (US), pages 33-54, XP002055686 see page 33, right-hand column, paragraph 4 see page 41, left-hand column, line 29 - right-hand column, line 30 see page 42, left-hand column, line 7 - line 12	1

☐ Further documents are listed in the continuation of box C

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of theinternational search	Date of mailing of the international search report
13 February 1998	27/02/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Intern nal Application No
PCT/EP 97/05081

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9421066 A	15-09-94	AU 683646 B	20-11-97
		AU 6255694 A	26-09-94

INTERNATIONALER RECHERCHENBERICHT

Intern nales Aktenzeichen
PCT/EP 97/05081

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

—

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 94 21066 A (TELSTRA) 15.September 1994 siehe Seite 4, Zeile 6 - Zeile 15 siehe Seite 6, Zeile 10 - Zeile 17 siehe Seite 7, Zeile 17 - Seite 8, Zeile 3	1,2
A	JUENEMAN ET AL.: "MESSAGE AUTHENTICATION WITH MANIPULATION DETECTION CODES" PROCEEDINGS OF THE 1983 SYMPOSIUM ON SECURITY AND PRIVACY, 25.April 1983, SILVER SPRING (US), Seiten 33-54, XP002055686 siehe Seite 33, rechte Spalte, Absatz 4 siehe Seite 41, linke Spalte, Zeile 29 - rechte Spalte, Zeile 30 siehe Seite 42, linke Spalte, Zeile 7 - Zeile 12	1

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
13.Februar 1998	27/02/1998

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Intern. Aktenzeichen
PCT/EP 97/05081

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9421066 A	15-09-94	AU 683646 B	20-11-97
		AU 6255694 A	26-09-94